1967

Regular p-groups

Joan Gary Taylor
Lehigh University

Regular p-Groups

by

Joan Gary Taylor

A Thesis
Presented to the Graduate Faculty
of Lehigh University
in Candidacy for the Degree of
Master of Science

Lehigh University
1967

This thesis is accepted and approved in partial fulfillment of the requirements for the degree of Master of Science.

September 15, 1967
Date

Albert W. Otto
Professor in Charge

Everett Pitcher
Head of the Department

Table of Contents

ABSTRACT

The concept and basic theory of regular p-groups was introduced by Philip Hall in March, 1932, in his paper "A Contribution to the Theory of Groups of Prime-power Order". Since that time not only Philip Hall, but also J. L. Alperin, C. Hobby, Otto Grün, and P.M. Weichel have studied regular p-groups. This thesis is a collection of the main results in this field.

Chapter 1 describes P. Hall's collecting process and the results flowing from it which motivated the notion of regular p-groups. In Chapter 2 we examine sufficient conditions for p-groups to be regular. We use W. R. Scott's proof to show one of the most important of these conditions, which is that for every a and b in a p-group G there exists a c in $\langle a,b\rangle$[1] such that $(ab)^p = a^p b^p c^p$. Also in Chapter 2 we show the following results of P. Hall: if G is a regular p-group, then the p^αth powers of elements of G form a subgroup $\mho_\alpha$, and the order of the product of any number of elements of G cannot exceed the orders of all the factors. Thus the elements of a regular p-group whose orders divide p^α form a subgroup Ω_α. All results in Chapter 3 are due to P. Hall. The essence of this chapter is the definition of the invariant μ for a regular p-group as well as the following theorem. The order p^{ω_α} of $\Omega_\alpha/\Omega_{\alpha-1}$ is

equal to the order of $\mho_{\alpha-1}/\mho_{\alpha}$ for each $\alpha = 1,\ldots,\mu$. Further, the invariants ω_{α} satisfy

$$\omega_1 \geq \omega_2 \geq \cdots \geq \omega_{\mu} .$$

Chapter 4 deals with the direct product of regular p-groups by giving conditions under which such a direct product is regular. Two of Grün's results, which we prove in this chapter, are as follows. For regular p-groups G_1 and G_2 where $G_1 \times G_2 = G$, G is regular if the classes of G_1 and G_2 are less than p or if G_2^1 has invariant 1 or 0.

NOTATION

To facilitate making references, definitions, lemmas, theorems, corollaries, and remarks are numbered consecutively with respect to each of the four chapters. Thus 3.5 refers to the third chapter, fifth numbered paragraph. We shall give credit for a lemma or theorem by placing the author's name in parentheses following the word lemma or theorem. Roman and Arabic numerals in parentheses and *'s only have significance in the numbered paragraph in which they are introduced. The letter p will always denote a prime, and each of α and n will denote a positive integer, unless otherwise stated. By the class of a group G, we mean the nilpotent class. In this paper we are discussing finite groups only. The following notation will be used.

$\langle a, b\rangle$ is the group generated by a and b.

G^1 is the derived group of the group G.

$x^y = y^{-1}xy$ where x and y are group elements.

e is the identity element of a group.

$o(G)$ denotes the order of a group G.

$\mathcal{N}$ denotes the positive integers.

$A \subset B$ means A is properly contained in B.

$A \subseteq B$ means A is contained in B.

$a | b$ means a divides b where a and b are integers.

$\mho_\alpha(G) = \{x^{p^\alpha} : x \text{ is in } G\}$ where G is a p-group and α is a non-negative integer.

$\Omega_\alpha(G) = \{x \text{ in } G : o(x) \mid p^\alpha\}$ where G is a p-group, and α is a non-negative integer.

$\sum_{i=1}^{r} B_i$ denotes the direct sum of the groups B_i, $i = 1,\ldots,r$.

$N(A)$ denotes the normalizer of the subgroup A of a group.

$G \times H$ denotes the internal direct product of the subgroups G and H.

CHAPTER 1

HALL's COLLECTING PROCESS

1.1 Definitions. Let $G = \langle a_1, \ldots, a_r \rangle$. Then $(a_i, a_j) = a_i^{-1} a_j^{-1} a_i a_j$ is called the (simple) commutator of a_i and a_j. We shall write

(1) $((b_1, b_2), b_3) = (b_1, b_2, b_3)$

and inductively

(2) $((b_1, \ldots, b_{n-1}), b_n) = (b_1, \ldots, b_n)$

where each b_j is an a_i, $i = 1, \ldots, r$. The above are called simple commutators on $a_1, \ldots, a_r$. The components of (1) and (2) are b_1, b_2, b_3 and $b_1, \ldots, b_n$ respectively. We now define by recurrence what we mean by a complex commutator of weight ω in the components $a_1, a_2, \ldots, a_r$. The complex commutators of weight 1 are the elements $a_1, a_2, \ldots, a_r$ themselves. Assuming that all complex commutators of weight less than ω have already been defined, we define those of weight ω to be all the expressions of the form (c_i, c_j) where c_i and c_j are any complex commutators of weights ω_1 and ω_2 in the components $a_1, a_2, \ldots, a_r$ respectively such that $\omega_1 + \omega_2 = \omega$. An example of a complex commutator is

$$*((a_1, a_2), (a_3, a_4, a_5)).$$

Throughout the rest of this chapter by a commutator we shall mean a complex commutator on $a_1,\ldots,a_r$ only. Since we are thus restricting our commutators, their components will be the a_i's, $i = 1,\ldots,r$. Consequently the weight of such a commutator is simply the number of a_i's, $i = 1,\ldots,r$, involved in it's expression. For example the weight of $*$ is five.

1.2 Remarks. It is possible that as group elements $((a_1,a_2),a_3) = ((a_1,a_2),\ (a_3,a_4))$; however, we shall not consider them equal as commutators. As commutators (c_i,c_j) is the same as (c_s,c_t) if and only if $c_i = c_s$ and $c_j = c_t$. Thus there is no ambiguity in our definition of weight of a commutator.

We order the commutators by

(i) $a_1,\ldots,a_r$ are simply ordered by the rule $a_1 < a_2 <\ldots< a_r$ and

(ii) commutators of wieght n will follow all commutators of weight less than n, and for weight n, $(c_i,c_j) < (c_k,c_\ell)$ if $c_j < c_\ell$ or if c_j and c_ℓ are the same commutators and $c_i < c_k$.

Our objective is to develop a formula for $(a_1a_2\ldots a_r)^n$ in terms of commutators. We first observe that for any two commutators c and d

$$** \ cd = dc\ (c,d).$$

Now $(a_1 \ldots a_r)^n = (a_1 \ldots a_r)(a_1 \ldots a_r) \ldots (a_1 \ldots a_r)$, n-times. To avoid confusion of terms we write the right hand side as

$$a_1(1)a_2(1) \ldots a_r(1)a_1(2)a_2(2) \ldots a_r(2) \ldots a_r(n).$$

Applying ** we have

$(a_1a_2 \ldots a_r)^n = a_1(1)a_2(1) \ldots a_{r-1}(1)a_1(2)a_r(1)(a_r(1), a_1(2))a_2(2) \ldots a_r(n)$. Hence we have moved $a_1(2)$ one place to the left and introduced a commutator $(a_r(1), a_1(2))$. In this manner we continue to move $a_1(2)$ to the left until it is next to $a_1(1)$. We then move $a_1(3)$ to the left until it is next to $a_1(2)$, and we continue until we have moved all the a_1's to the far left. This completes the first stage of collection. The proceedure is known as the collecting process. We now collect in order $a_2(1), a_2(2), \ldots, a_2(n)$ immediately to the right of a_1's and thus complete the second stage of collection. At the end of the <u>ith</u> stage we have

$$\text{***} \quad (a_1a_2 \ldots a_r)^n = c_1^{e_1} c_2^{e_2} \ldots c_i^{e_i} \; R_1R_2 \ldots R_t,$$

where $c_1, c_2, \ldots, c_i$ are the first i commutators and $R_1, \ldots, R_t$ are commutators later than c_i in the ordering. Observe that some commutators will not appear. If $R_{j_1}, R_{j_2}, \ldots, R_{j_s}$ are in order from left to right the commutators among $R_1, \ldots, R_t$ which are c_{i+1}, we apply ** to move R_{j_1} to the position immediately to the right of $c_i^{e_i}$. We then move $R_{j_2}, \ldots, R_{j_s}$. Thus with $e_{i+1} = s$

*** becomes

$$(a_1a_2\dots a_r)^n = c_1^{e_1}c_2^{e_2}\dots c_{i+1}^{e_{i+1}}\ T_1\dots T_k .$$

where $T_1,\dots,T_k$ are commutators later than c_{i+1} in the ordering. This is the $i+1$ th stage.

Although P. Hall introduced the collecting process, the source of the above discussion, as well as the following theorem and corollary, is M. Hall. By presenting the collecting process formally, we could have set up the machinery needed to prove the theorem in this chapter; however, the theorem is too far removed from regularity. We are mainly interested in it's corollary.

1.3 Theorem (M. Hall). Let $G = \langle a_1,\dots,a_r\rangle$. The product $(a_1a_2\dots a_r)^n$ may be collected in the form

$$(a_1a_2\dots a_r)^n = a_1^n a_2^n \dots a_r^n c_{r+1}^{e_{r+1}}\dots c_i^{e_i} R_1\dots R_t$$

where $c_{r+1},\dots,c_i$ are commutators on $a_1,\dots,a_r$ in order, and $R_1,\dots,R_t$ are commutators on $a_1,\dots,a_r$ later than c_i in the ordering. For $1 \le j \le i$, $e_j = b_1n + b_2n^{(2)}+\dots+b_mn^{(m)}$ where m is the weight of c_j, the b's are non-negative integers which depend only on c_j, and $n^{(k)} = n(n-1)\dots(n-k+1)/k!$.

1.4 Corollary (M. Hall). If G is a p-group of class less than p, then with $n = p^\alpha$

$$(a_1a_2\dots a_r)^n = a_1^n a_2^n \dots a_r^n S_1^n \dots S_t^n$$

where $S_1, S_2, \ldots, S_t$ belong to $\langle a_1, \ldots, a_r \rangle^1$.

Proof. From the theorem we have

$$(a_1 \ldots a_r)^n = a_1^n \ldots a_r^n \, c_{r+1}^{e_{r+1}} \ldots c_i^{e_i} R_1 \ldots R_t \, .$$

where we have collected all commutators of weight less than p. Then the R_ℓ, $\ell = 1, \ldots, t$, are of weight at least p and thus belong to at least the pth member of the lower central series of G. Since G has class less than p, this is just the identity. Moreover, with $n = p^\alpha$ the exponents e_j, $j = r+1, \ldots, i$, are multiples of p^α since $n^{(\beta)}$, $\beta \leq p-1$, is a binomial coefficient such that the numerator contains n as a factor but the denominator contains factors not exceeding $p-1$. That is to say, e_j is a sum of terms each of which contains n as a factor.

CHAPTER 2

BASIC PROPERTIES

2.1 Definition. A p-group G is said to be regular if for any two elements a and b of G and α in $\mathcal{N}$, we have

$$(ab)^{p^{\alpha}} = a^{p^{\alpha}} b^{p^{\alpha}} x_1^{p^{\alpha}} \cdots x_t^{p^{\alpha}}$$

where $x_1, \ldots, x_t$ are in $\langle a, b\rangle^1$.

2.2 Theorem. (i) (M. Hall). Every p-group of class less than p is regular.

(ii) (M. Hall). Every p-group of order at most p^p is regular.

(iii) (M. Hall). A p-group G is regular if every subgroup generated by two elements in G is regular.

(iv) (M. Hall). Every subgroup and factor group of a regular p-group is regular.

(v) (Scott). An Abelian p-group is regular.

(vi) (Grün). Every p-group whose elements other than e are all of order p is regular.

Proof. (i) follows from 1.4.

(ii) follows from (i) since a group of order at most p^p has class less than p.

(iii), (v), (vi), and the first part of (iv) follow from the definition.

We now prove the second partof (iv) by showing that the homomorphic image of a regular p-group is regular. Let a and b be members of the regular p-group G. Then $(ab)^{p^\alpha} = a^{p^\alpha} b^{p^\alpha} x_1^{p^\alpha} \ldots x_r^{p^\alpha}$ where the x_i's, $i = 1,\ldots,r$, belong to $\langle a,b\rangle^1$. Let T be a homomorphism of G, and apply it to the above statement. Then we have

$$T((ab)^{p^\alpha}) = T(a^{p^\alpha} b^{p^\alpha} x_1^{p^\alpha} \ldots x_r^{p^\alpha})$$

where $T(x_i)$ is in $T(\langle a,b\rangle^1)$. But this is the same as

$$(T(a)T(b))^{p^\alpha} = (T(a))^{p^\alpha}(T(b))^{p^\alpha}(T(x_1))^{p^\alpha} \ldots (T(x_r))^{p^\alpha}$$

where $T(x_i)$ is in $T(\langle a,b\rangle^1) = (T(\langle a,b\rangle))^1 = \langle T(a),T(b)\rangle^1$.

2.3 Theorem (Scott). If G is a finite 2-group, then G is regular if and only if G is Abelian.

Proof. If G is Abelian, then it is regular. Conversely, suppose that G is a regular non-Abelian 2-group of least order. If $o(G^1) > 2$, then G^1 contains a subgroup H normal in G of order two. If G/H were Abelian, then $G^1 \subseteq H$. So G/H is non-Abelian and regular which contradicts the minimality of G. Hence $o(G^1) = 2$. By regularity $(ab)^2 = a^2b^2x_1^2 \ldots x_t^2$ where x_i, $i=1,\ldots,t$, is in $\langle a,b\rangle^1$. Thus $(ab)^2 = a^2b^2$ since x_i is in G^1 which has order two. Then G is Abelian. This is a contradiction.

2.4 Theorem (P. Hall). If G is a regular p-group, then the product of the p^{α}th powers of two or more elements of G is itself the p^{α}th power of some element of G.

Proof. It is enough to show that if a and b are in G, then there exists a c in G such that $a^{p^{\alpha}}b^{p^{\alpha}} = c^{p^{\alpha}}$ because the result for a product of more than two p^{α}th powers will follow by repeated applications.

Case 1. G is Abelian. Then $c = ab$ willsuffice.

Case 2. G is non-Abelian. We suppose the theorem holds for every proper subgroup of G and argue by induction over the order of G. Regularity implies $a^{p^{\alpha}}b^{p^{\alpha}} = x_r^{\,p^{\alpha}} \cdots x_2^{\,p^{\alpha}} x_1^{\,p^{\alpha}} (ab)^{p^{\alpha}}$ where each x_i, $i=1,\ldots,r$, is in $\langle a,b\rangle^1$. Thus the x_i's are in G^1. Hence $L = \langle ab, x_1, \ldots, x_r\rangle \subseteq \langle ab, G^1\rangle$. Because G is non-Abelian, $\langle ab, G^1\rangle$ is a proper subgroup since G^1 is a subgroup of the Frattini subgroup of G, and thus all it's members are non-generators of G. So L is a proper subgroup of G, and the theorem holds for L. Thus there exists a c in L such that $a^{p^{\alpha}}b^{p^{\alpha}} = c^{p^{\alpha}}$.

2.5 Remarks. If G is a regular p-group, 2.4 proves that the set of p^{α}th powers of elements of G form a subgroup of G. This subgroup is denoted $\mho_{\alpha}(G)$ or $\mho_{\alpha}$ when it is clear as to what group we are referring. This is easily seen to be a characteristic subgroup of G.

2.6 Theorem (Scott). Let G be a p-group. Of the conditions

(i) G is regular,

(ii) for all a and b in G, there exists a c in $\langle a,b\rangle^1$ such that $(ab)^p = a^p b^p c^p$, and

(iii) if H is a subgroup of G, then $\mho_n(H)$ is a subgroup of G and $[\mho_n(H)]^1$ is a subgroup of $\mho_n(H^1)$,

either (i) or (ii) implies the other two.

Proof. We assume that G is of least order such that the theorem is false and aim for a contradiction. Then G is a group where either (i) holds and one of (ii) or (iii) does not hold or (ii) holds and one of (i) or (iii) does not hold. If either (i) or (ii) holds for G, then (i), (ii), and (iii) hold for all proper subgroups of G by our assumption.

Case 1. Suppose (ii) holds. Let H be a subgroup of G. We show that (iii) holds by induction on n for both parts.

We first show that $\mho_n(H)$ is a subgroup of G. Let a and b be in H. For $n = 1$ we wish to show $a^p b^p$ is in $\mho_1(H)$. Without loss of generality we may let $H = \langle a,b\rangle$ since if $a^p b^p$ is in $\mho_1(\langle a,b\rangle)$, then $a^p b^p$ in $\mho_1(H)$. If H is cyclic, then $a^p b^p = (ab)^p$ which is in $\mho_1(H)$. Suppose H is not cyclic. Then (ii) implies there exists a c in H^1

so that $a^p b^p = (ab)^p c^p$. As in the proof of 2.4 H^1 is contained in the Frattini subgroup of H, and so $\langle ab, c\rangle \subset H$. Thus (iii) holds for $\langle ab, c\rangle$, and there exists a d in $\langle ab, c\rangle$ so that $(ab)^p c^p = d^p$. Then $a^p b^p = d^p$ where d is in H, and the proposition holds for $n = 1$. We now assume $\mho_n(H)$ is a subgroup of G. Since the proposition is true for $n = 1$, we have $\mho_1(\mho_n(H))$ is a subgroup of G. But $\mho_1(\mho_n(H)) = \mho_{n+1}(H)$. Thus the proposition holds for $n + 1$.

We now show that $[\mho_n(H)]^1$ is a subgroup of $\mho_n(H^1)$. Let a and b be in H. For $n = 1$ we wish to show (a^p, b^p) is in $\mho_1(H^1)$. Without loss of generality we may let $H = \langle a, b\rangle$ since if (a^p, b^p) is in $\mho_1(\langle a, b\rangle^1)$, then (a^p, b^p) is in $\mho_1(H^1)$. By (ii) we have

(a) there exists a d in H^1 such that
$(a^{-1})^p (b^{-1})^p = d^p (a^{-1}b^{-1})^p$,

(b) there exists a c in H^1 such that
$a^p b^p = (ab)^p c^p$, and

(c) there exists a g in $\langle a^{-1}b^{-1}, ab\rangle^1 \subseteq H^1$
such that $(a^{-1}b^{-1})^p (ab)^p = (a^{-1}b^{-1}ab)^p g^p$.

Since $H^1 \subseteq G^1 \subset G$, H^1 is regular, and there exists an f in H^1 such that $d^p (a^{-1}b^{-1}ab)^p g^p c^p = f^p$. By (a), (b), and (c) we have

$$\begin{aligned}(a^p, b^p) &= a^{-p}b^{-p}a^pb^p \\ &= (a^{-1})^p(b^{-1})^p a^pb^p \\ &= d^p(a^{-1}b^{-1})^p(ab)^pc^p \\ &= d^p(a^{-1}b^{-1}ab)^pg^pc^p \\ &= f^p.\end{aligned}$$

Thus (a^p, b^p) is in $\mho_1(H^1)$, and so the proposition holds for $n = 1$. We now assume $[\mho_n(H)]^1$ is a subgroup of $\mho_n(H^1)$, and prove that $[\mho_{n+1}(H)]^1$ is a subgroup of $\mho_{n+1}(H^1)$. Since the proposition holds for $n = 1$, we have

$$[\mho_1(\mho_n(H))]^1 \subseteq \mho_1([\mho_n(H)]^1).$$

Thus $$\begin{aligned}[\mho_{n+1}(H)]^1 &= [\mho_1(\mho_n(H))]^1 \\ &\subseteq \mho_1([\mho_n(H)]^1) \\ &\subseteq \mho_1(\mho_n(H^1)) \\ &\subseteq \mho_{n+1}(H^1).\end{aligned}$$

This proves (iii).

We now show (i) holds by induction on n. Let a and b be in G. For the case $n = 1$ (ii) implies $(ab)^p = a^pb^pc^p$ where c is in $\langle a,b\rangle^1$. We assume $(ab)^{p^n} = a^{p^n}b^{p^n}x_1^{p^n}\ldots x_r^{p^n}$ where x_i, $i=1,\ldots,r$, is in $\langle a,b\rangle^1$ and prove that $(ab)^{p^{n+1}} = a^{p^{n+1}}b^{p^{n+1}}y_1^{p^{n+1}}\ldots y_t^{p^{n+1}}$ where $y_i, i=1,\ldots,t$, is in $\langle a,b\rangle^1$. Since $\langle a,b\rangle^1 \subseteq G^1 \subset G$, $\langle a,b\rangle^1$ is regular and there exists a c in $\langle a,b\rangle^1$ such that $x_1^{p^n}x_2^{p^n}\ldots x_r^{p^n} = c^{p^n}$. So

$$
\begin{aligned}
(ab)^{p^{n+1}} &= ((ab)^{p^n})^p \\
&= (a^{p^n} b^{p^n} x_1{}^{p^n} \ldots x_r{}^{p^n})^p \\
&= (a^{p^n} b^{p^n} c^{p^n})^p.
\end{aligned}
$$

Now (ii) implies there exists a d in $\langle a^{p^n}, b^{p^n} c^{p^n}\rangle^1$ such that $(a^{p^n} b^{p^n} c^{p^n})^p = (a^{p^n})^p (b^{p^n} c^{p^n})^p d^p$

$$= a^{p^{n+1}} (b^{p^n} c^{p^n})^p d^p.$$

Since d is in $\langle a^{p^n}, b^{p^n} c^{p^n}\rangle^1$, d is in $[\mho_n(\langle a,b\rangle)]^1$. Also (ii) implies there exists a g in $\langle b^{p^n}, c^{p^n}\rangle^1 \subseteq [\mho_n(\langle a,b\rangle)]^1$ such that $(b^{p^n} c^{p^n})^p = (b^{p^n})^p (c^{p^n})^p g^p$

$$= b^{p^{n+1}} c^{p^{n+1}} g^p.$$

Finally $[\mho_n(\langle a,b\rangle)]^1 \subseteq \mho_n(\langle a,b\rangle^1)$ implies there exist x and y in $\langle a,b\rangle^1$ such that $d = x^{p^n}$ and $g = y^{p^n}$. Then we have

$$(ab)^{p^{n+1}} = a^{p^{n+1}} b^{p^{n+1}} c^{p^{n+1}} x^{p^{n+1}} y^{p^{n+1}}$$

where c, x, and y are in $\langle a,b\rangle^1$. Thus (i) holds. So if (ii) holds, then we have that (i) and (iii) must hold. Hence (i) must hold and one of (ii) and (iii) does not.

Case 2. Suppose (i) holds. Then (ii) holds for let a and b be in G. By (i) there exist $x_1, \ldots, x_r$ in $\langle a,b\rangle^1$ such that $(ab)^p = a^p b^p x_1{}^p \ldots x_r{}^p$... But $\mho_1(\langle a,b\rangle^1)$ is a subgroup; hence, there exists a c in $\langle a,b\rangle^1$ such that $x_1{}^p \ldots x_r{}^p = c^p$. Thus

$(ab)^p = a^p b^p c^p$ for c in $\langle a,b\rangle^1$. So (ii) holds. By Case 1 (ii) holds implies (iii) holds, and we have that G is a group such that (i), (ii), and (iii) hold. This is a contradiction.

2.7 Theorem (P. Hall). Let G be a regular p-group and a and b be any two members of G. Then it is always possible to find elements $x_1, x_2, \ldots, x_s$ in $\langle a,c\rangle^1$ where $c = (a,b)$ such that $(a^{p^\alpha}, b) = c^{p^\alpha} x_1^{p^\alpha} \ldots x_s^{p^\alpha}$.

Proof. Regularity implies that $(ac)^{p^\alpha} = a^{p^\alpha} c^{p^\alpha} x_1^{p^\alpha} \ldots x_s^{p^\alpha}$ where x_i, $i=1,\ldots,s$, is in $\langle a,c\rangle^1$. But $(ac)^{p^\alpha} = (aa^{-1}b^{-1}ab)^{p^\alpha} = (b^{-1}ab)^{p^\alpha} = b^{-1}a^{p^\alpha}b$. Thus

$$\begin{aligned}(a^{p^\alpha}, b) &= a^{-p^\alpha} b^{-1} a^{p^\alpha} b \\ &= a^{-p^\alpha} a^{p^\alpha} c^{p^\alpha} x_1^{p^\alpha} \ldots x_s^{p^\alpha} \\ &= c^{p^\alpha} x_1^{p^\alpha} \ldots x_s^{p^\alpha}\end{aligned}$$

2.8 Lemma. If $K = \langle a,b\rangle$, then $K^1 = \langle k^{-1}(a,b)k : k \text{ is in } K\rangle$.

Proof. (a,b) is in K^1 which is normal in K. Therefore, $\langle k^{-1}(a,b)k : k \text{ is in } K\rangle \subseteq K^1$. Now any two elements k_1 and k_2 of K may be expressed as $x_1 \ldots x_m$ and $y_1 \ldots y_n$ respectively where m and n are in $\mathcal{N}$ and x_i and y_j are a or b. Thus a generator of K^1 has the form $(x_1 \ldots x_m, y_1 \ldots y_n) = \pi(x_i, y_j)^{k_{ij}}$ where

x_i and y_j are a or b and k_{ij} is in K. The order of the factors is arbitrary, but k_{ij} depends on the order. Thus every member of K^1 is a member of $\langle k^{-1}(a,b)k\colon\ k \text{ is in } K\rangle$.

2.9 Theorem (P. Hall). Let G be a regular p-group, and let a and b be in G. Then

(i) $(a^{p^\alpha}, b) = e$ if and only if $(a,b)^{p^\alpha} = e$,

(ii) if a^{p^α} is the least power of a to be permutable with b, then b^{p^α} is the least power of b to be permutable with a,

(iii) the order of (a,b) cannot exceed the orders of either a or b relative to the center of $\langle a,b\rangle$,

(iv) the order of any complex commutator of weight greater than 1 and containing the element a as a component can never exceed the order of a relative to the center of G, and

(v) the order of the product of any number of elements of G cannot exceed the orders of all the factors.

Proof. Before proving this theorem we would like to show a fact which will be used several times in the proof. Let L be a regular p-group which is generated by two elements y_1 and y_2, and assume 2.9 holds for L.

If x is in L^1, then $o(x) \leq o(y_1)$. For by 2.8, we have $L^1 = \langle \ell^{-1}(y_1,y_2)\ell : \ell \text{ is in } L\rangle$. By (iii) of 2.9 we have $o((y_1,y_2)) \leq o(y_1)$ relative to the center of L, and thus $o((y_1,y_2)) \leq o(y_1)$. Hence $o(\ell^{-1}(y_1,y_2)\ell) \leq o(y_1)$ for each ℓ in L. If x is in L^1, then x is a product of conjugates of (y_1,y_2) each with order less than or equal to $o(y_1)$, and so by (v) of 2.9 $o(x) \leq o(y_1)$.

Since the theorem is true when G is Abelian, we assume that G is non-Abelian. We will argue by induction on the order of G and assume 2.9 is true for every proper subgroup of G.

We first prove (i). By 2.7

$$*(a^{p^\alpha},b) = c^{p^\alpha} x_1{}^{p^\alpha} \ldots x_s{}^{p^\alpha}$$

where $c = (a,b)$ and $x_1,\ldots,x_s$ are in $\langle a,c\rangle^1$. Suppose $(a,b)^{p^\alpha} = e$. Let $L = \langle a,c\rangle$. Since L is a proper subgroup of G, the theorem holds for L by assumption. Therefore, $o(x_i) \leq o(c)$ for $i = 1,\ldots,s$, and thus $x_i{}^{p^\alpha} = e$. Then $*$ becomes $(a^{p^\alpha},b) = e$.

Conversely, suppose $(a^{p^\alpha},b) = e$. Then a^{p^α} lies in the center of $K = \langle a,b\rangle$ and thus in the center of $L = \langle a,c\rangle$ where $c = (a,b)$. Again L is a proper subgroup of G, and so $o(x_i) \leq o(a)$ relative the center of L, where $i=1,\ldots,s$. Thus $o(x_i) \leq p^{\alpha}$, and $x_i^{p^{\alpha}} = e$. Then * becomes $e = c^{p^{\alpha}}$. So (i) is proven. Observe that a consequence of (i) is that the order of (a,b) is equal to the order of a relative to the center of $\langle a,b\rangle$.

We now prove (ii). Suppose p^{α} is the least power of a to be permutable with b, and so $(a^{p^{\alpha}},b) = e$. Then by (i) we have $(a,b)^{p^{\alpha}} = e$. Since $o((a,b)) = o((b,a))$, we have $(b,a)^{p^{\alpha}} = e$. Then by (i) $(b^{p^{\alpha}},a) = e$. Let $p^{\beta} < p^{\alpha}$. If $b^{p^{\beta}}$ were to permute with a, then $(b^{p^{\beta}},a) = e$ which implies $(b,a)^{p^{\beta}} = e$ which implies $(a,b)^{p^{\beta}} = e$ which implies $(a^{p^{\beta}},b) = e$. This is a contradiction.

We now prove (iii). This follows from (i), for let p^{α} be the order of (a,b), and let β be a non-negative integer such that $\beta < \alpha$. If $(a^{p^{\beta}},b) = e$, then $(a,b)^{p^{\beta}} = e$, which is a contradiction. Since $o((a,b)) = o((b,a))$, the proof is complete.

We now prove (iv). Proof is by induction on the weight n of a complex commutator. The case $n = 2$ is (iii). We assume the proposition is true for weights less than or equal to n and seek to prove it for $n + 1$. Let c be a complex commutator of weight $n + 1$ containing a as a component. Then c is an expression of the form (c_1, c_2) where c_1 or c_2 is a complex commutator of weight less than or equal to n and containing a as a component, say c_1. Then (iii) implies $o((c_1, c_2)) \leq o(c_1)$ relative to the center of $\langle c_1, c_2 \rangle$. Thus $o((c_1, c_2)) \leq o(c_1)$ relative to the center of G. The induction hypothesis implies $o(c_1) \leq o(a)$ relative to the center of G. Consequently, $o((c_1, c_2)) \leq o(a)$ relative to the center of G.

It remains to prove (v). Since G is regular, we have

$$** (ab)^{p^\alpha} = a^{p^\alpha} b^{p^\alpha} x_1^{p^\alpha} \cdots x_r^{p^\alpha}$$

where the x_i, $i=1, .., r$, are in $\langle a, b \rangle^1$. Let p^β denote the max $\{o(a), o(b)\}$, and let $K = \langle a, b \rangle$. By the remarks preceeding the proof of 2.9 there exists a set of generators of K^1 such that none has order exceeding the order of a. Since $K^1 \subset G$, no element in K^1 has order exceeding the order of a. Thus $o(x_i) \leq o(a) \leq p^\beta$. Then $x_i^{p^\beta} = e$, and ** gives $(ab)^{p^\beta} = e$. By repeated applications we see that the order of a product of elements of G cannot exceed the orders of all the factors.

2.10 Example (M. Hall). We now give an example of a p-group which is not regular. Consider the symmetric group S_{p^2} on p^2 letters.

Let $a_1 = (1,2,\ldots,p)$,

$$a_2 = (p+1, p+2, \ldots, 2p),$$

$$\vdots$$

$$a_i = ((i-1)p+1,\ (i-1)p+2, \ldots, ip),$$

$$\vdots$$

$$a_p = ((p-1)p+1,\ (p-1)p+2, \ldots, pp).$$

Let $A = \langle a_i : i=1,\ldots,p\rangle$. Now $o(a_i) = p$, and the a_i's are disjoint, and so $a_i a_j = a_j a_i$. Thus A is an elementary Abelian p-group. Hence A is the direct sum of cyclic groups each of order p.

Thus $o(A) = p^p$ since $A = \sum_{i=1}^{p} \langle a_i\rangle$. Let

$$b = (1, p+1, 2p+1, \ldots, p^2-p+1)(2, p+2, \ldots p^2-p+2)\ldots(p, 2p, \ldots, p^2).$$

Then $o(b) = p$. Let $B = \langle b\rangle$.

We first show that AB is a subgroup of order p^{p+1}. By simple multiplication we see that $b^{-1}a_ib = a_{i+1}$ where the subscripts are taken modulo p. Thus b is in $N(A)$ and so $B \subseteq N(A)$. Therefore, AB is a subgroup of S_{p^2}. Since members of A and B are products of disjoint cycles, and no member of A contains a cycle equal to a cycle in a member of B, it is impossible for A and B to have a permutation in common other than the identity. Thus $A \cap B = e$. Therefore $o(AB) = p^{p+1}$.

We now show that AB is a p-group which is not regular. First we show that AB has an element of order p^2. Consider $(ba_1)^{p^2}$. From $b^{-1}a_ib = a_{i+1}$ we have $a_ib = ba_{i+1}$, and so

$$
\begin{aligned}
(ba_1)^p &= (ba_1)(ba_1)\dots(ba_1) \quad \text{(p times)} \\
&= ba_1ba_1ba_1ba_1ba_1\dots ba_1 \\
&= bba_2ba_2ba_2ba_2\dots ba_2a_1 \\
&= bbba_3ba_3ba_3\dots ba_3a_2a_1 \\
&= bbbba_4ba_4\dots ba_4a_3a_2a_1 \\
&= bbbbba_5\dots ba_5a_4a_3a_2a_1 \\
&\;\;\vdots \\
&= b^pa_pa_{p-1}\dots a_1.
\end{aligned}
$$

Since the a_i's commute and have order p and since $b^p = e$, we have $(ba_1)^{p^2} = [(ba_1)^p]^p$

$$=[b^p a_p \cdots a_1]^p$$

$$= [a_p \cdots a_1]^p$$

$$= [a_p^p a_{p-1}^p \cdots a_1^p]$$

$$= e.$$

Now the product $a_p \cdots a_1$ is not e since the a_i's are disjoint. Thus $o(ba_1) = p^2$. Recall that a_1 and b both have order p. Thus if AB were regular, $o(ba_1) \leq p$ by 2.9. But $o(ba_1) = p^2$; thus AB is not regular.

2.11 Theorem (P. Hall). Let a and b be in a regular p-group G. If $a^{p^\alpha} = b^{p^\alpha}$, then $(ab^{-1})^{p^\alpha} = e$ and conversely.

Proof. Suppose $a^{p^\alpha} = b^{p^\alpha}$. By regularity we have

$$(ab^{-1})^{p^\alpha} = a^{p^\alpha} (b^{-1})^{p^\alpha} x_1^{p^\alpha} \cdots x_s^{p^\alpha} = x_1^{p^\alpha} \cdots x_s^{p^\alpha}$$

where x_i, $i=1,\ldots,s$, belongs to the derived group of $K = \langle a,b^{-1}\rangle = \langle a,b\rangle$. Since $b^{p^\alpha} = a^{p^\alpha}$, b^{p^α} commutes with powers of a and of b, and so

b^{p^α} belongs to the center of K. By the opening remarks in the proof of 2.9 $o(x_i) \leq o(b)$ relative to the center of K, and thus $o(x_i) \leq p^\alpha$. Then $x_i^{p^\alpha} = e$, $i=1,\ldots,s$, and we have $(ab^{-1})^{p^\alpha} = e$.

Now suppose $(ab^{-1})^{p^\alpha} = e$. Let $t = ab^{-1}$; then $a^{p^\alpha} = (tb)^{p^\alpha} = t^{p^\alpha} b^{p^\alpha} y_1^{p^\alpha} \ldots y_r^{p^\alpha} = b^{p^\alpha} y_1^{p^\alpha} \ldots y_r^{p^\alpha}$ where $y_1,\ldots,y_r$ belong to the derived group of $K = \langle t,b\rangle = \langle a,b\rangle$. Again by the remarks preceeding the proof of 2.9 $o(y_i) \leq o(t) \leq p^\alpha$, $i=1,\ldots,r$. Thus $y_i^{p^\alpha} = e$, and so $a^{p^\alpha} = b^{p^\alpha}$.

CHAPTER 3
INVARIANTS

In this chapter G is a regular p-group, and α and β are non-negative integers.

3.1 Definition. We denote by p^{μ} the highest order of any element of G. μ is an invariant of G, written μ or $\mu(G)$.

3.2 Definition. By 2.9(v) the set of elements of G whose orders divide p^{α} is a subgroup. This subgroup is denoted $\Omega_{\alpha}(G)$ or Ω_{α}. It is clearly a characteristic subgroup of G.

3.3 Remarks. Since G possesses an element of order p^{μ} but none of order $p^{\mu+1}$, we have

(1) $G = {}_{o}\quad {}_{1} \cdots {}_{\mu-1}\quad {}_{\mu} = e,$

$G = {}_{\mu}\quad {}_{\mu-1} \cdots {}_{1}\quad {}_{o} = e,$

(2) $\mho_{\alpha} \subseteq \Omega_{\mu-\alpha}$ $(\alpha = 0,1,\ldots,\mu)$, and

$\mho_{a-1} \nsubseteq \Omega_{\mu-\alpha}$ $(\alpha = 1,2,\ldots,\mu)$.

The first expression of (2) is true since for $x^{p^{\alpha}}$ in $\mho_{\alpha}$ we have $[x^{p^{\alpha}}]^{p^{\mu-\alpha}} = x^{p^{\mu}} = e$. To verify the second expression of (2) simply pick an element

y in G whose order is p^{μ}. Then $y^{p^{\alpha-1}}$ is in $\mho_{\alpha-1}$, but $[y^{p^{\alpha-1}}]^{p^{\mu-\alpha}} = y^{p^{\mu-1}} \neq e$, and so $y^{p^{\alpha-1}}$ is not in $\Omega_{\mu-\alpha}$. Thus (2) again expresses that p^{μ} is the highest order of an element of G.

For $\alpha = 0, 1, \ldots, \mu-\beta$ we have

$$\mu(\mho_{\alpha}/\mho_{\alpha+\beta}) = \mu(\Omega_{\alpha+\beta}/\Omega_{\alpha}) = \beta$$

since $[\mho_{\alpha+\beta}x^{p^{\alpha}}]^{p^{\beta}} = \mho_{\alpha+\beta}$ and $[\Omega_{\alpha}y]^{p^{\beta}} = \Omega_{\alpha}$, where x is in G and y is in $\Omega_{\alpha+\beta}$.

3.4 Lemma (P. Hall). $\Omega_{\alpha+\beta}(G) = \left\{x : x\Omega_{\beta} \text{ is in } \Omega_{\alpha}(G/\Omega_{\beta})\right\}$.

Proof. Suppose x is in $\Omega_{\alpha+\beta}(G)$. Then $x^{p^{\alpha+\beta}} = e$, and so $(x^{p^{\alpha}})^{p^{\beta}} = e$. Thus $x^{p^{\alpha}}$ is in Ω_{β}. Then $x^{p^{\alpha}}\Omega_{\beta} = \Omega_{\beta}$; that is, $(x\Omega_{\beta})^{p^{\alpha}} = \Omega_{\beta}$. Therefore $x\Omega_{\beta}$ is in $\Omega_{\alpha}(G/\Omega_{\beta})$. Conversely, let x be a member of G such that $x\Omega_{\beta}$ is in $\Omega_{\alpha}(G/\Omega_{\beta})$. Then $(x\Omega_{\beta})^{p^{\alpha}} = \Omega_{\beta}$; that is, $x^{p^{\alpha}}\Omega_{\beta} = \Omega_{\beta}$. Thus $x^{p^{\alpha}}$ is in Ω_{β}. Therefore $(x^{p^{\alpha}})^{p^{\beta}} = e$, and x is in $\Omega_{\alpha+\beta}(G)$.

3.5 Lemma (P. Hall). $o(\Omega_\alpha/\Omega_{\alpha-1}) = o(\mathcal{U}_{\alpha-1}/\mathcal{U}_\alpha)$ for $\alpha = 1,\ldots,\mu$ if and only if $o(\mathcal{U}_\alpha) = o(G/\Omega_\alpha)$ for $a = 1,\ldots,\mu$.

Proof. Suppose $o(\Omega_\alpha/\Omega_{\alpha-1}) = o(\mathcal{U}_{\alpha-1}/\mathcal{U}_\alpha)$ for $\alpha = 1,\ldots,\mu$. The proof is by induction on α. First we consider the case $\alpha = 1$. $o(\Omega_1/\Omega_o) = o(\mathcal{U}_o/\mathcal{U}_1)$ implies that $o(\mathcal{U}_1) = o(\mathcal{U}_o)\, o(\Omega_o)/o(\Omega_1)$. That is, $o(\mathcal{U}_1) = o(G/\Omega_1)$ by (1) of 3.3. We assume $o(\mathcal{U}_\alpha) = o(G/\Omega_\alpha)$ and will prove $o(\mathcal{U}_{\alpha+1}) = o(G/\Omega_{\alpha+1})$. We have that

$$\begin{aligned} o(\mathcal{U}_\alpha) &= o(G)/o(\Omega_\alpha) \\ &= o(G)/o(\Omega_{\alpha+1}) \quad o(\Omega_{\alpha+1})/o(\Omega_\alpha) \\ &= o(G)/o(\Omega_{\alpha+1}) \quad o(\mathcal{U}_\alpha)/o(\mathcal{U}_{\alpha+1}). \end{aligned}$$

Thus

$$\begin{aligned} o(\mathcal{U}_{\alpha+1}) &= o(G)/o(\Omega_{\alpha+1}) \quad o(\mathcal{U}_\alpha)/o(\mathcal{U}_\alpha) \\ &= o(G)/o(\Omega_{\alpha+1}). \end{aligned}$$

Now suppose $o(\mathcal{U}_\alpha) = o(G/\Omega_\alpha)$ for $\alpha = 1,\ldots,\mu$. Then $o(\mathcal{U}_{\alpha-1})o(\Omega_{\alpha-1}) = o(G)$ for $\alpha = 1,\ldots,\mu$ since the only case different than the assumptions is $o(\mathcal{U}_0)o(\Omega_0)$ which by (1) of 3.3 is $o(G)$. Hence

$$o(\mathcal{U}_{\alpha-1})o(\Omega_{\alpha-1}) = o(G) = o(\mathcal{U}_\alpha)o(\Omega_\alpha)$$

and so

$$o(\Omega_\alpha/\Omega_{\alpha-1}) = o(\mathcal{U}_{\alpha-1}/\mathcal{U}_\alpha).$$

3.6 Theorem (P. Hall). The order p^{ω_α} of $\Omega_\alpha/\Omega_{\alpha-1}$ is equal to the order of $\mathcal{U}_{\alpha-1}/\mathcal{U}_\alpha$ for each $\alpha = 1,\ldots,\mu$. Further, the invariants ω_α satisfy

$$\omega_1 \geq \omega_2 \geq \cdots \geq \omega_\mu .$$

Proof. For g in G $\Omega_\alpha g = \left\{x \text{ in } G\colon\ gx^{-1} \text{ is in } \Omega_\alpha\right\}$; that is, all x such that $(gx^{-1})^{p^\alpha} = e$. By 2.11 this implies that $g^{p^\alpha} = x^{p^\alpha}$. So the elements of any coset of Ω_α in G all have the same p^α th power. Conversely, if two elements of G have the same p^αth power, they belong to the same coset of Ω_α. Thus the number of p^αth powers is equal to the number of cosets of Ω_α. Hence for $\alpha = 1,\ldots,\mu$ we have $o(G/\Omega_\alpha = o(\mathcal{U}_\alpha)$ and so $o(\Omega_\alpha/\Omega_{\alpha-1}) = o(\mathcal{U}_{\alpha-1}/\mathcal{U}_\alpha)$.

For the second part of the theorem it suffices to prove that $\omega_1 \geq \omega_2$ or that $o(\Omega_2/\Omega_1)$ does not exceed $o(\Omega_1)$.

The reason is if we apply this result to G/Ω_β, we have

$$o(\Omega_2(G/\Omega_\beta)/\Omega_1(G/\Omega_\beta)) \leq o(\Omega_1(G/\Omega_\beta)/\Omega_o(G/\Omega_\beta)).$$

that is, $o(\Omega_{\beta+2}(G)/\Omega_{\beta+1}(G)) \leq o(\Omega_{\beta+1}(G)$ which says $p^{\omega_{\beta+2}} \leq p^{\omega_{\beta+1}}$ or $\omega_{\beta+1} \geq \omega_{\beta+2}$.

We now show $o(\Omega_2/\Omega_1) \leq o(\Omega_1)$. We may assume $\mu(G) \geq 2$ since otherwise there is nothing to prove. Now $\mu(\Omega_2) = 2$. Hence by (2) of 3.3.

$$\mho_1(\Omega_2) \subseteq \Omega_{2-1}(\Omega_2) = \Omega_1(\Omega_2) = \Omega_1(G) = \Omega_1.$$

Thus $o(\Omega_2/\Omega_1) \leq o(\Omega_2/\mho_1(\Omega_2))$. But by the first part of the theorem, which says $o(\Omega_\alpha)/o(\mho_{\alpha-1}) = o(\Omega_{\alpha-1})/o(\mho_\alpha)$, we have $o(\Omega_2(\Omega_2))/o(\mho_1(\Omega_2)) = o(\Omega_1(\Omega_2))/o(\mho_2(\Omega_2))$. But $\mu(\Omega_2) = 2$, so $\mho_2(\Omega_2) = e$, and $\Omega_2(\Omega_2) = \Omega_2$. Then

$$o(\Omega_2/o(\mho_1(\Omega_2)) = o(\Omega_1(\Omega_2)) = o(\Omega_1).$$

Thus we have $o(\Omega_2/\Omega_1) \leq o(\Omega_1)$.

CHAPTER 4

DIRECT PRODUCTS

4.1 Remarks. Throughout this chapter by direct product we shall mean internal direct product. As a matter of convenience, we shall also speak of the (internal) direct product of two groups G_1 and G_2 when actually we may be referring to $G_1^* \times G_2^*$ where G_1^* is isomorphic to G_1 and G_2^* is isomorphic to G_2.

That the direct product of regular p-groups is not necessarily a regular p-group is shown by P. M. Weichsel. In this chapter we will discuss conditions under which the direct product of regular p-groups is regular.

4.2 Lemma (Grün). Let G_1 and G_2 be regular p-groups with $G = G_1 \times G_2$. Every simple commutator of weight n in G is the product of a simple commutator of weight n in G_1 with a simple commutator of weight n in G_2.

Proof. Every element in G may be represented by a product $ab = ba$ where a is in G_1 and b is in G_2. Then for $a_1, \ldots, a_n$ in G_1 and $b_1, \ldots, b_n$ in G_2 we have

$$\begin{aligned}(a_1b_1, a_2b_2) &= (a_1b_1)^{-1}(a_2b_2)^{-1}a_1b_1a_2b_2\\ &= a_1^{-1}b_1^{-1}a_2^{-1}b_2^{-1}a_1b_1a_2b_2\\ &= a_1^{-1}a_2^{-1}a_1a_2b_1^{-1}b_2^{-1}b_1b_2\\ &= (a_1, a_2)(b_1, b_2).\end{aligned}$$

Hence it follows by induction that

$$(a_1b_1, a_2b_2, \ldots, a_nb_n) = (a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n).$$

4.3 Theorem (Grün). Let G_1 and G_2 be regular p-groups. The direct product of G_1 and G_2 is regular if the classes of G_1 and G_2 are smaller than p.

Proof. A simple commutator in G_1 and G_2 which has weight greater than or equal to p is e. A simple commutator in G of weight greater than or equal to p is the product of a simple commutator of weight greater than or equal to p in G_1 with a simple commutator of weight greater than or equal to p in G_2 and hence is e. Thus the class of G is less than p.

4.4 Theorem (Grün). Let G_1 and G_2 be regular p-groups with $G = G_1 \times G_2$. If $G_2{}^1$ has invariant 1 or 0, then G is regular.

Proof. Let a_1b_1 and a_2b_2 be arbitrary elements in G, where a_1 and a_2 are in G_1 and b_1 and b_2 are in G_2. Now $(b_1b_2)^{p^\alpha} = b_1^{p^\alpha}b_2^{p^\alpha}$. Hence

$$\begin{aligned}(a_1b_1a_2b_2)^{p^\alpha} &= (a_1a_2)^{p^\alpha}(b_1b_2)^{p^\alpha}\\ &= a_1^{p^\alpha}a_2^{p^\alpha}x_1^{p^\alpha}\ldots x_s^{p^\alpha}b_1^{p^\alpha}b_2^{p^\alpha}\end{aligned}$$

where $x_1,\ldots,x_s$ are in $\langle a_1,a_2\rangle^1$. As a result of this we have

$$*(a_1b_1a_2b_2)^{p^\alpha} = (a_1b_1)^{p^\alpha}(a_2b_2)^{p^\alpha}x_1^{p^\alpha}\ldots x_s^{p^\alpha}$$

where $x_1,\ldots,x_s$ are in $\langle a_1,a_2\rangle^1$. Now $x_i, i=1,\ldots,s$, is a product of commutators; that is, $x_i = c_1c_2\ldots c_t$ where $c_j = (w_1,w_2)$ for $j=1,\ldots,t$ and w_1 and w_2 are words in a_1 and a_2. Let $\bar{w}_1$ and $\bar{w}_2$ be corresponding words in b_1 and b_2, and let $\bar{c}_j = (\bar{w}_1,\bar{w}_2)$ for $j=1,\ldots,t$. Let $z_i = \bar{c}_1\bar{c}_2\ldots\bar{c}_t$. Thus z_i is in $\langle b_1,b_2\rangle^1$. If $y_i = x_iz_i$, then y_i is in $\langle a_1b_1,a_2b_2\rangle^1$. Therefore, $y_i^{p^\alpha} = x_i^{p^\alpha}z_i^{p^\alpha} = x_i^{p^\alpha}$ since $\mu(G_2^1)$ is 1 or 0. Thus * becomes

$$(a_1b_1a_2b_2)^{p^\alpha} = (a_1b_1)^{p^\alpha}(a_2\ b_2)^{p^\alpha}y_1^{p^\alpha}\ldots y_s^{p^\alpha}\quad,$$

and thus G is regular by definition.

4.5 Corollary (Grün). The direct product of a regular p-group with an Abelian p-group G_2 is regular.

Proof. Whenever G_2 is Abelian, $\mu(G_2{}^1) = 0$.

4.6 Corollary (Grün). The direct product of a regular p-group with a p-group G_2 whose invariant is 1 is regular.

Proof. Whenever $\mu(G_2) = 1$, $\mu(G_2{}^1) \leq 1$.

4.7 Theorem (Grün). Let G_1 and G_2 be regular p-groups. If $G = G_1 \times G_2$, then the factor groups $G/\mho_1(G_1{}^1)$ and $G/\mho_1(G_2{}^1)$ are regular.

Proof. $(G_1/\mho_1(G_1{}^1))^1 = G_1{}^1/\mho_1(G_1{}^1)$ which has invariant 1. Also $G/\mho_1(G_1{}^1)$ is isomorphic to $G_1/\mho_1(G_1{}^1) \times G_2$ under the map i, where i carries $G_1/\mho_1(G_1{}^1) \times G_2$ to $G/\mho_1(G_1{}^1)$ and is defined by

$$i[(\mho_1(G_1{}^1)x)y] = \mho_1(G_1{}^1)\ (xy)$$

for x in G_1 and y in G_2. That i is an isomorphism is immediate. Thus by 4.4 $G/\mho_1(G_1{}^1)$ is regular. An analogous proof holds for $G/\mho_1(G_2{}^1)$.

4.8 Theorem (Grün). Let G_1 and G_2 be regular p-groups $G_1 \times \Omega_1(G_2)$ and $\Omega_1(G_1) \times G_2$ are regular normal subgroups of $G = G_1 \times G_2$.

Proof. It follows from the definition that $\Omega_1(G_1)$ and $\Omega_1(G_2)$ have invariant 1.

4.9 Lemma (Alperin). Let G be a p-group, when p is odd, such that every 2 generator subgroup of G has a cyclic derived group. Then G is regular.

Proof. Let a and b be in G. By 2.6 it suffices to show there exists a k in $\mathcal{N}$ such that $(ab)^p = a^p b^p (a,b)^{kp}$. Let $H = \langle a,b \rangle$. Then H^1 is cyclic and so H has class at most two. It then follows from 2.8 that $H^1 = \langle (a,b) \rangle$. The derived group of $H/\mho_1(H^1)$ is $H^1/\mho_1(H^1)$ and, therefore, has invariant 1 and so order p. Then $H/\mho_1(H^1)$ is of class 2 and is, therefore, regular since p is odd. By regularity we have

$$\mho_1(H^1)(ab)^p = \mho_1(H^1)a^p b^p (\mho_1(H^1)c)^p$$

$$= \mho_1(H^1)\, a^p b^p$$

where c is in H^1 and so c^p is in $\mho_1(H^1)$. Thus $(ab)^p = a^p b^p$ modulo $\mho_1(H^1)$. Since $(a,b)^p$ generates $\mho_1(H^1)$, we are done.

4.10 Lemma (Alperin). Let J be a 3-group such that

(i) J can be generated by two elements,

(ii) J satisfies the identical relation $(xy)^3 = x^3y^3$, and

(iii) every element of J^1 has order at most three.

Then J is of class at most two.

Proof. First we show that J has class at most three. To do this we use an induction argument on $o(J)$ and so assume the lemma is true for all 3-groups satisfying (i), (ii), and (iii) and having order less than the order of J. Suppose the class of J is greater than or equal to four. Let $K = J/J_3$, where J_3 is the fourth member of the lower central series of J and thus $J_3 \neq e$. Then $o(K) < o(J)$, and also K satisfies (i), (ii), and (iii). Then by the induction hypothesis the class of K is less than or equal to two. That is, class $(J/J_3) \leq 2$. We then have $K_2 = J_2/J_3 = e$. This implies that $J_2 = J_3$ which is a contradiction. Thus we have shown that J has class at most three.

If a and b are in J where $\langle a,b\rangle = J$, then

$$a^3b^3 = (ab)^3 = ababab$$
$$= a^2b(b,a)bab$$

$$= a^3b(b,a)^2(b,a,a)b(b,a)b$$

$$= a^3b^2(b,a)^2(b,a,b)^2(b,a,a)(b,a)b$$

$$= a^3b^3(b,a)^2(b,a,b)^4(b,a,a)(b,a)(b,a,b).$$

Since the class of J is at most three, commutators in a and b of weight at least three belong to the center of J. Thus by (iii) we have

$$a^3b^3 = a^3b^3(b,a)^3(b,a,b)^5(b,a,a)$$

$$= a^3b^3(b,a,b)^2(b,a,a).$$

Therefore

$$*(b,a,b)^2(b,a,a) = e$$

Replacing b by b^2 yields

$$a^3b^6 = (ab^2)^3 = abbabbabb$$

$$= abab(b,a)bab(b,a)bb$$

$$= aab(b,a)b(b,a)ab(b,a)b(b,a)bb$$

$$= a^2b(b,a)ba(b,a)(b,a,a)b(b,a)b(b,a)bb$$

$$= a^2b(b,a)ab(b,a)^2(b,a,a)b(b,a)b(b,a)bb$$

$$= a^2ba(b,a)(b,a,a)b(b,a)^2(b,a,a)b(b,a)$$
$$b(b,a)bb$$

$$= a^2ab(b,a)^2b(b,a,a)(b,a)^2(b,a,a)$$
$$b(b,a)b(b,a)bb$$

$$= a^3b(b,a)b(b,a)(b,a,b)(b,a,a)$$
$$(b,a)^2b(b,a,a)(b,a)b(b,a)bb$$

$$= a^3bb(b,a)(b,a,b)(b,a)(b,a,b)(b,a)b$$
$$(b,a)b(b,a)(b,a,b)(b,a,a)b(b,a)$$
$$(b,a,b)b(b,a)(b,a,b)b$$

$$= a^3b^3(b,a,b)^2(b,a,a)(b,a)b(b,a,b)$$
$$(b,a,a)(b,a)b(b,a,b)(b,a)b(b,a,b)$$

$$= a^3b^3(b,a,b)^2(b,a,a)b(b,a)(b,a,b)^2$$
$$(b,a,a)b(b,a)(b,a,b)^2b(b,a)(b,a,b)^2$$

$$= a^3b^4(b,a,a)(b,a)b(b,a,a)(b,a)b(b,a,b)^2$$
$$(b,a)$$

$$= a^3b^4(b,a,a)b(b,a)(b,a,b)(b,a,a)$$
$$b(b,a)(b,a,b)^3(b,a)$$

$$= a^3b^5(b,a,a)^2(b,a)b(b,a,b)(b,a)^2$$

$$= a^3b^5(b,a,a)^2b(b,a)(b,a,b)^2(b,a)^2$$

$$= a^3b^6(b,a,a)^2(b,a,b)^2.$$

Thus we have

$$**(b,a,a)^2(b,a,b)^2 = e.$$

It follows from *,**, and (iii) that $(b,a,a) = (b,a,b) = e$. Consequently (a,b) is in the center of J. Thus for each j in J $j^{-1}(a,b)j$ is in the center of J, and so J^1 is in the center of J. Therefore, the class of J is two.

4.11 Lemma (Alperin). If H is any regular 3-group which can be generated by two elements, then H^1 is cyclic.

Proof. Let u and v be in H. By regularity we have

$$(uv)^3 = u^3v^3w^3$$

where w is in $\langle u,v\rangle^1$ and so w^3 is in $\mho_1(H^1)$. Hence the group $H/\mho_1(H^1)$ satisfies the identical relation $(xy)^3 = x^3y^3$, that is, 4.10(ii). $H/\mho_1(H^1)$ also satisfies (i) and (iii) of 4.10 and thus has class at most two. Now let a and b be members of $H/\mho_1(H^1)$ such that $H/\mho_1(H^1) = \langle a,b\rangle$. Then by 2.8 $H^1/\mho_1(H^1) = \langle g^{-1}(a,b)g : g \text{ is in } H/\mho_1(H^1)\rangle$. Since $H/\mho_1(H^1)$ has class at most two, $H^1/\mho_1(H^1)$ is in the center of $H/\mho_1(H^1)$. Thus $H^1/\mho_1(H^1) = \langle (a,b)g^{-1}g : g \text{ is in } H/\mho_1(H^1)\rangle = \langle (a,b)\rangle$. Since $H^1/\mho_1(H^1)$ is cyclic and $\mho_1(H^1)$ is contained in the Frattini subgroup of H^1, H^1 is cyclic.

4.12 Theorem (Alperin). If G is a regular 3-group, then $G \times H$ is regular for all regular 3-groups H if and only if G^1 has invariant at most 1.

Proof. Suppose G^1 has invariant 1. Then 4.4 implies that $G \times H$ is regular.

Suppose by way of contradiction that $\mho_1(G^1) \neq e$. Let g_1 and g_2 be elements of G. such that $(g_1,g_2)^3 \neq e$. As a consequence of 4.11 and 2.8 $\langle g_1,g_2\rangle^1 = \langle (g_1,g_2)\rangle$. Now (g_1,g_2,g_1) is in $\langle g_1,g_2\rangle^1$, and so there exists an m in $\mathcal{N}$ with $m \not\equiv 0$ modulo 3 such that $(g_1,g_2,g_1) = (g_1,g_2)^{m3^\alpha}$. Let H be the group generated by h_1 and h_2 with relations

$$h_1^{3^{\alpha+1}} = h_2^{3^{\alpha+1}} = (h_1,h_2)^{3^{\alpha+1}} = e \quad ,$$

$$(h_1,h_2,h_2) = e \quad , \quad \text{and}$$

$$(h_1,h_2,h_1) = (h_1,h_2)^{-m3^\alpha} .$$

It can be checked that H is a 3-group. Furthermore by 4.9 it is regular. To see this let $\langle a_1,a_2\rangle \subseteq H$. Now $\langle a_1,a_2\rangle = \langle h_{i_1}h_{i_2}\cdots h_{i_u}, h_{i_1}\cdots h_{i_v}\rangle$ where $i=1$ or 2 and u and v are in $\mathcal{N}$. Let x be in $\langle a_1,a_2\rangle^1$. Then $x = \pi(a_{i_1}\cdots a_{i_q}, a_{i_1}\cdots a_{i_r})$ where

$i=1$ or 2 and q and r are in $\mathcal{N}$. Thus $x = \pi(h_{i_1}\ldots h_{i_s}h_{i_1}\ldots h_{i_t})$ where $i=1$ or 2 and s and t are in $\mathcal{N}$. Let y be a factor of x. Then $y = \pi(h_i,h_j)^{h_{ij}}$ where $i,j=1$ or 2 and the h_{ij} are in H. We then have

$$*y = \pi(h_i,h_j)^{h_{i_1}\ldots h_{i_z}}$$

where $i = 1$ or 2 and z is in $\mathcal{N}$. But $(h_1,h_2,h_2) = e$ implies $h_2^{-1}(h_1,h_2)h_2 = (h_1,h_2)$ or $(h_1,h_2)^{h_2} = (h_1,h_2)$. Also $(h_1,h_2,h_1) = (h_1,h_2)^{-m3^\alpha}$ implies $(h_1,h_2)^{h_1} = (h_1,h_2)^{-m3^\alpha+1}$. We can let $i=1$ and $j=2$ in $*$ since $(h_2,h_1) = (h_1,h_2)^{-1}$. Using these latter relations to reduce $*$, we see that $y = (h_1,h_2)^d$ where d is in $\mathcal{N}$. Thus $x = \pi(h_1,h_2)^d = (h_1,h_2)^f$ where f is in $\mathcal{N}$. Thus any 2-generator subgroup of H has a cyclic derived group and so H is regular.

Now consider the subgroup K of $G \times H$ generated by g_1h_1, and g_2h_2 where g_1 and g_2 are in G and h_1 and h_2 are in H. Then by 4.2

$$(g_1h_1,g_2h_2) = (g_1,g_2)(h_1,h_2)$$

and

$$(g_1h_1,g_2h_2,g_1h_1) = (g_1,g_2,g_1)(h_1,h_2,h_1)$$

$$=(g_1,g_2)^{m3^\alpha}(h_1,h_2)^{-m3^\alpha}$$

If K^1 were cyclic, then $K^1 = \langle(g_1h_1,g_2h_2)\rangle$ $= \langle(g_1,g_2)(h_1,h_2)\rangle$. Thus $(g_1,g_2)^{m3^\alpha}(h_1,h_2)^{-m3^\alpha} =$ $[(g_1,g_2)(h_1,h_2)]^\beta = (g_1,g_2)^\beta(h_1,h_2)^\beta$ where β is a non-negative integer. Unique representation implies $m3^\alpha = \beta = -m3^\alpha$. Since $m \not\equiv 0$ modulo 3, this is impossible. Thus K^1 is not cyclic, and therefore $G \times H$ is not regular.

Bibliography

Alperin, J.L. "On a Class of Regular p-Groups." Transaction of the American Mathematical Society, 106 (1963), 77-99.

Grün, Otto. "Über das direkte Produkt regulärer p-Gruppen." Archiv der Mathematik, V(1954), 241-243.

Hall, Marshall. The Theory of Groups. New York: Macmillan, 1959.

Hall, Philip, "A Contribution to the Theory of Groups of Prime-power Order." Proceedings of the London Mathematical Society, 36 (1933), 29-95.

Hobby, Charles. "A Characteristic Subgroup of a p-Group." Pacific Journal of Mathematics, 10(1960), 853-858.

Scott, W. R. Group Theory. Englewood Cliffs, New Jersey: Prentice-Hall, 1964.

Weichsel, P.M. "Regular p-Groups and Varieties." Mathematishe Zeitschrift, 95 (1967), 223-231.

VITA

On April 1, 1943, Joan Gary Taylor was born to Joseph S. and Gertrude H. Gary in New Castle, Pennsylvania. She grew up in a small western Pennsylvania village called Enon Valley and in 1961 was graduated from the local high school. While attending Westminster College, New Wilmington, Pennsylvania, she belonged to the following national honor societies: Cwens, Mortarboard, Kappa Delta Pi, Delta Phi Alpha, and Kappa Mu Epsilon. In June, 1965, she was graduated cum laude, and in September of that year she came to Lehigh University, Bethlehem, Pennsylvania, as a Fellow-in-Teaching. It was at Lehigh University that she and her husband, John, met. They were married September 3, 1966. Mrs. Taylor plans to teach until her husband earns a Doctor of Philosophy degree.